

Claims

- [1] An apparatus for generating random numbers using digital logic, comprising:
a shift register which sequentially moves bit values stored therein;
a feedback circuit which performs a predetermined logic operation on the bit values stored in the shift register to generate a feedback signal;
an external signal generation circuit which generates an external signal input to the shift register; and
an input logic circuit which performs a predetermined logic operation on the feedback signal and the external signal and inputs a result of operation to the shift register.
- [2] The apparatus of claim 1, further comprising a fixed value prevention circuit that generates a signal with a value that allows an output of the input logic circuit to have a different value to a value of an output of the shift register and inputs the generated signal to the input logic circuit, when a logic value of the external signal is equivalent to all the bit values stored in the shift register.
- [3] The apparatus of claim 2, wherein the signal output from the fixed value prevention circuit is at logic high.
- [4] The apparatus of claim 1, wherein the external signal generation circuit generates a random signal.
- [5] The apparatus of claim 4, wherein the random signal is generated by sampling a sampled signal generated by a source that is different from a source of a sampling signal.
- [6] The apparatus of claim 5, wherein sampling is performed both at rising and falling edges of the sampling signal generated by a source that is different from a source of the sampled signal.
- [7] A method of generating random numbers using digital logic, comprising:
(a) sequentially moving bit values stored in a shift register;
(b) performing a predetermined logic operation on the bit values stored in the shift register to generate a feedback signal;
(c) generating an external signal input to the shift register; and
(d) performing a predetermined operation on the feedback signal and the external signal and inputting a result of the operation to the shift register.
- [8] The method of claim 7, wherein during (d), the predetermined logic operation is further performed on an output of a fixed value prevention circuit that allows the

result of the predetermined logic operation to be different to the bit values of the shift register, when a logic value of the external signal is equivalent to all the bit values stored in the shift register.

- [9] The method of claim 8, wherein the output of the fixed value prevention circuit is at logic high.
- [10] The method of claim 7, wherein the external signal is a random signal.
- [11] The method of claim 10, wherein the random signal is generated by sampling a sampled signal generated by a source that is different from a source of a sampling signal.
- [12] The method of claim 11, wherein sampling is performed both at rising and falling edges of the sampling signal generated by a source that is different from a source of the sampled signal.